デスクトップ マネジメントについて
HP Business PC

デスクトップ マネジメントについて

HP Business PC

改訂第 3 版：2009 年 9 月

製品番号：581009-291

このガイドについて

このガイドでは、一部のモデルにプリインストールされているセキュリティ機能とマネジメント機能の概念および使用手順について説明します。

警告！ その指示に従わないと、人体への傷害や生命の危険を引き起こすおそれがあるという警告事項を表します。

注意： その指示に従わないと、装置の損傷やデータの損失を引き起こすおそれがあるという注意事項を表します。

注記： 重要な補足情報です。

目次

1　デスクトップ マネジメントの概要

HP Client Management Solutions は、ネットワーク環境にあるデスクトップ、ワークステーション、およびノートブック コンピューターの管理と制御の分野で、標準のソリューションを提供しています。HP はデスクトップ マネジメントのパイオニアとして 1995 年に、デスクトップを完全に管理できる業界初のパーソナル コンピューターを世に送り出しました。HP はマネジメント機能の特許を取得しています。以来、デスクトップ、ワークステーション、およびノートブック コンピューターの効果的な導入、設定、および管理に必要な標準化とインフラストラクチャの開発において業界全体の取り組みをリードしてきました。HP は独自の管理ソフトウェアを開発し、業界トップ クラスの管理ソフトウェア ソリューション提供企業との提携関係によって、これらの企業の製品と HP Client Management Solutions の互換性を確保しています。HP Client Management Solutions は、ライフサイクル全体を通した PC の所有および管理の総費用削減に役立つソリューションを提供する幅広い取り組みの中でも重要な位置を占めるものです。

デスクトップ マネジメントの主要な機能と特長は、以下のとおりです。

- 出荷時設定の変更
- リモート システム インストール
- ソフトウェア アップデートおよびマネジメント機能
- ROM フラッシュ機能
- ハードウェア オプションの構成
- 資産情報管理機能およびセキュリティ機能
- 障害通知および復旧機能

注記：　このガイドで説明される機能のサポートについては、機種またはソフトウェアのバージョンによって異なることがあります。

2 出荷時設定の変更

お使いのコンピューターには、システム ソフトウェア イメージがプリインストールされています。短時間のソフトウェアの設定手順が終われば、すぐにコンピューターを使用できます。

プリインストールされたソフトウェア イメージの代わりにカスタマイズされたシステム ソフトウェアおよびアプリケーション ソフトウェアを使用することもできます。カスタマイズされたソフトウェア イメージを展開するには、いくつかの方法があります。

- プリインストールされたソフトウェア イメージを展開した後、追加するアプリケーションをインストールする
- [HP Client Automation]の Standard Edition や[HP Client Automation]の Enterprise Edition（Radia テクノロジ ベース）などのソフトウェア導入用ツールを使用して、プリインストールされているソフトウェア イメージをカスタマイズされたソフトウェア イメージで置き換える
- ディスク複製手順を使用して、ハードディスク ドライブの内容を別のハードディスクにコピーする

最適なコンピューター環境の構築方法は、お使いの情報技術環境や作業内容によって異なります。

ROM からのセットアップ、および ACPI ハードウェアによって、システム ソフトウェアのリストア、コンフィギュレーション マネジメント機能、トラブルシューティング、および省電力機能を利用することができます。

HP Client Automation Agent

[HP Client Automation]の Standard Edition および Enterprise Edition の両方で使用する管理エージェントは、コンピューターにプリロードされています。このエージェントをインストールすると、HP 管理コンソールとの通信が可能になります。

[HP Client Automation Agent]をインストールするには、以下の操作を行います。

1. **[スタート]**をクリックします。
2. **[すべてのプログラム]**をクリックします。
3. **[HP Manageability]**（HP 管理）をクリックします。
4. 希望する言語に該当する**[HP Management Agent Readme]**をクリックします。
5. Readme ファイルに記載されている手順を確認し、それに沿って[HP Client Automation Agent]をインストールします。

[HP Client Automation Agent]は、[HP Client Automation]ソリューションすべてを有効にするための主要なインフラストラクチャ コンポーネントです。HP Configuration Management Solution の実行に必

要なその他のインフラストラクチャ コンポーネントについて詳しくは、http://h20229.www2.hp.com/solutions/ascm/index.html（英語サイト）を参照してください。

HP Client Manager

[HP Client Manager]（HPCM）は、Symantec 社が開発した無料の製品であり、サポートされているすべての HP のビジネス向けデスクトップ コンピューター、ノートブック、ワークステーション、および HP Blade PC で使用できます。HPCM は、[HP System Software Manager]、[HP インスタント サポート・プロフェッショナル・エディション]、[HP Client Management Interface]などの HP 固有のツールを統合し、サポートされているすべての HP ハードウェアの集中的な管理、追跡、監視を可能にします。

[HP Client Manager 7.0]は、ワンストップショップとして機能する新しいポータルページを特色とし、管理者は以下の管理タスクを実行できます。

- インベントリ
- アラート
- BIOS の管理
- ドライバーの更新
- [HP Instant Support Health Scan]および Diagnostics の実行
- Embedded Security タスクを実行する
- 過去 3 ～ 6 か月の HP システム状態アラートの傾向を包括的に表示する
- [HP Instant Support Health Scan]および Diagnostics で、サポートされているコンピューターの準拠について包括的に表示する
- HP コンピューターの概要を表示する：サポートされている各種デスクトップ、ノートブック、ワークステーションおよび HP Blade PC の分析
- アラートの表示：アセット、しきい値、ハードウェア状態
- レポート
- HP 固有のツールを更新する管理タスク

HPCM は http://www.symantec.com/business/theme.jsp（英語サイト）からダウンロードできます。**[Strategic Partner Products]**の下の**[HP Client Manager]**をクリックしてください。無料の永続的なライセンスをダウンロードページから取得することもできます。

また、HPCM の操作手順に関するビデオが http://www.symantec.com/connect/（英語サイト）で公開されています。**[HP Client Manager 7.0]**で検索すると、HPCM 内の各種タスクについて手順を追って説明したビデオを表示できます。

3 リモート システム インストール

リモート システム インストール機能を使用すると、[Preboot Execution Environment]（PXE）を起動することにより、ネットワーク サーバー上のソフトウェアや設定情報を使ってシステムを起動したりセットアップしたりできます。リモート システム インストールの機能は、通常、システム セットアップやコンフィギュレーションのためのツールとして使用しますが、以下のような場合にも使用できます。

- ハードディスク ドライブをフォーマットする場合
- 1 台以上の新しいコンピューターにソフトウェア イメージを導入する場合
- フラッシュ ROM を使用してシステム BIOS をリモートでアップデートする場合（14 ページの 「リモート ROM フラッシュ機能」を参照）

  注記： Microsoft® Windows®オペレーティングシステム内からシステム BIOS をフラッシュする機能があります。

- システム BIOS を設定する場合

リモート システム インストールを起動するには、起動時に表示される HP ロゴの画面の右下隅に**[F12 = Network Service Boot]**と表示されたら、すぐに F12 キーを押します。画面のメッセージに従って、リモート システム インストールを起動します。初期設定の起動順序は BIOS のコンフィギュレーションの設定ですが、常に PXE を起動するように変更できます。

4 ソフトウェアのアップデートと管理

HP では、デスクトップ コンピューター、ワークステーション、およびノートブック コンピューターのソフトウェアを管理し、アップデートするための以下のツールを提供しています。

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools セキュリティ マネージャー
- [HP Client Automation]の Starter Edition、Standard Edition、および Enterprise Edition
- HP Client Manager from Symantec
- Altiris Client Management Suite
- HP Client Catalog for Microsoft System Center & SMS Products
- Active Management Technology 対応の Intel® vPro®搭載コンピューター
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

IT 部門で使用しているシステム管理ツールに関係なく、ハードウェア アセットとソフトウェア アセットの両方を管理することは、IT コストの削減とビジネスの迅速化にとって重要です。IT 管理者は簡単なスクリプトを作成して目的の管理ソリューションに組み込むことによって、HP Client Management Interface にアクセスできます。

HP Client Management Interface（HP CMI）を使用すると、HP ビジネス コンピューターはユーザーが管理する IT 環境とシームレスに統合されます。HP CMI は、HP ビジネス コンピューターと一般的なシステム管理ツール（[Microsoft Systems Management Server]、[IBM Tivoli Software]、および[HP Operations]を含む）および社内で開発した管理アプリケーションとの統合を簡略化するインタフェースを提供します。HP CMI を使用すると、システム管理ツールとアプリケーションが直接クライアント コンピューターと通信することで、詳細なクライアント インベントリを要求したり、システム状態情報を受信したり、システムの BIOS 設定を管理したりできます。その結果、エージェントやコネクタ ソフトウェアが統合を行う必要が少なくなります。

HP Client Management Interface は、Microsoft Windows Management Interface（MS WMI）、Web-Based Enterprise Management（WBEM）、System Management BIOS（SMBIOS）、および

Advanced Configuration and Power Interface（ACPI）などの業界標準に準拠しています。HP CMI は、HP Client Management Solutions で使用される基礎テクノロジです。HP CMI を使用すると、HP クライアント コンピューターの管理方法を柔軟に選択できるようになります。

HP Client Management Interface をシステム管理ソフトウェアと併用すると、以下のことが可能になります。

- 詳細なクライアント インベントリ情報の要求：プロセッサ、ハードディスク ドライブ、メモリ、BIOS、ドライバーなどに関する詳細情報を取得します。センサー情報（ファンの速さ、電圧、温度など）も含まれます。
- システム状態情報の受信：システム管理コンソール、アプリケーション、またはローカル クライアント コンピューターに対する幅広いクライアント ハードウェア警告（適正温度の超過、ファンの停止、ハードウェア構成の変更など）の送信を登録します。警告は、ハードウェア イベントによってトリガーされたときにリアルタイムで送信されます。
- システム BIOS 設定の管理：任意のまたはすべてのクライアント システム上のシステム管理コンソールから、各システムに移動することなくリモートで F10 機能（BIOS パスワードおよびコンピューターのブート順序の設定や変更など）を実行します。

HP Client Management Interface について詳しくは、http://www.hp.com/go/hpcmi/（英語サイト）を参照してください。

HP SoftPaq Download Manager

[HP SoftPaq Download Manager]は、お使いの環境で HP クライアント PC モデル用のソフトウェアの更新を見つけたりダウンロードしたりするための、無料の使いやすいインタフェースです。モデル、オペレーティング システム、言語を指定することで、必要な SoftPaq をすばやく見つけて並べ替え、選択することができます。[HP SoftPaq Download Manager]は http://www.hp.com/go/sdm/（英語サイト）からダウンロードできます。

HP System Software Manager

[HP System Software Manager]（SSM）は、ネットワーク上にある HP Business PC のデバイス ドライバーおよび BIOS アップデートのリモート展開を自動化するための、無料のユーティリティです。SSM を実行すると、各ネットワーク クライアント システムにインストールされているドライバーおよび BIOS のリビジョン レベルが（ユーザーとの対話なしに）自動的に確認され、このインベントリと、すでにテストされ、中央のファイル格納ディレクトリに格納されているシステム ソフトウェアの SoftPaq が比較されます。SSM では次に、ネットワーク PC 上の古いリビジョンのシステム ソフトウェアが、ファイル格納ディレクトリで使用可能な最新のレベルに自動的にアップデートされます。SSM では SoftPaq アップデートが正しいクライアント システム モデルにだけ配布されるため、管理者は確実かつ効率的に、SSM を使用してシステム ソフトウェアを最新版に維持できます。

[HP System Software Manager]は、[HP Client Automation]ソリューション、[HP Client Manager from Symantec]、[Microsoft Systems Management Server]（SMS）などのエンタープライズ ソフトウェア配布ツールと共に使用できます。SSM を使用すると、SSM 形式にパッケージ化された、顧客が作成したアップデートや他社製アップデートを配布できます。

SSM は、http://www.hp.com/go/ssm/（英語サイト）から無料でダウンロードできます。

注記： Windows BitLocker Drive Encryption が有効になっていて、TPM 測定を使用しているシステムでは、BIOS をフラッシュすると、BitLocker がプラットフォーム用に作成した信頼署名が無効になります。そのため、このようなシステムの場合、BitLocker キーを保護するために、SSM では現在リモート ROM フラッシュがサポートされていません。システム BIOS をフラッシュするには、グループ ポリシーで BitLocker を無効にしてください。

BIOS の TPM 測定を使用せずに BitLocker サポートを有効にすると、BitLocker キーが無効になることを防ぐことができます。緊急時にリカバリできるように、BitLocker 証明書をバックアップしておくことをおすすめします。

HP ProtectTools セキュリティ マネージャー

HP ProtectTools セキュリティのソフトウェアは、コンピューター本体、ネットワーク、および重要なデータを不正なアクセスから保護するために役立つセキュリティ機能を提供します。以下のソフトウェア モジュールによって高度なセキュリティ機能が提供され、[HP ProtectTools セキュリティ マネージャー]からその機能にアクセスできます。

[HP ProtectTools セキュリティ マネージャー]は単一のコンソールで、ここから他のすべてのモジュールにアクセスできます。

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java™ Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro for HP ProtectTools

HP ProtectTools では、2 つの種類を利用できます。[HP ProtectTools Security Manager]および[HP ProtectTools Administrative Console]です。管理者用バージョンもユーザー用バージョンも、**[スタート]→[すべてのプログラム]**メニューから利用できます。

コンピューターで利用可能なソフトウェアモジュールは、モデルによって異なる可能性があります。たとえば、Embedded Security for HP ProtectTools は、TPM（Trusted Platform Module）セキュリティ チップが内蔵されているコンピューターでのみ利用できます。

[HP ProtectTools]ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。一部の HP Pro デスクトップ コンピューターでは、[HP ProtectTools]は製品購入後にオプションとして導入できます。詳しくは、http://www.hp.com/jp/を参照してください。

[HP Client Automation]の Starter Edition および Standard Edition

[HP Client Automation]は、Windows Vista®、Windows XP、および HP Thin Client 環境向けのハードウェアおよびソフトウェア管理ソリューションです。このソリューションは使用しやすく導入が簡単

で、同時に将来的な要件に対応する強力な基盤も提供できます。以下の 2 つの種類で提供されています。

- Starter Edition は、HP のデスクトップ コンピューター、ノートブック コンピューター、およびワークステーションを管理するための無料の製品で、ハードウェアおよびソフトウェア インベントリ、リモート制御、HP アラート監視、HP BIOS およびドライバー アップデート、[HP Protect Tools]との統合、Intel AMT に対するアドオン サポートなどの機能を提供します。Starter Edition はまた、HP Thin Client の導入と管理もサポートします。
- 販売用製品である Standard Edition には、Starter Edition で提供されるすべての機能が含まれているほか、Windows の導入と移行、パッチ管理機能、ソフトウェア配布、およびソフトウェア使用率計測が追加されています。

[HP Client Automation]の Starter Edition および Standard Edition では、絶えず変化する、大規模で、種類の異なる IT 環境を自動的に管理するための、[HP Client Automation]の Enterprise Edition（Radia テクノロジ ベース）への移行パスが提供されます。

[HP Client Automation]ソリューションについて詳しくは、http://www.hp.com/go/client/（英語サイト）を参照してください。

[HP Client Automation]の Enterprise Edition

[HP Client Automation]の Enterprise Edition は、管理者が、種類の異なるクライアント プラットフォームにわたってソフトウェアとコンテンツのインベントリ管理、展開、パッチの適用、および連続的な管理を行うことができる、ポリシー ベースのソリューションです。[HP Client Automation]の Enterprise Edition を使用すると、IT 技術者は以下のことが行えるようになります。

- 検出、導入から、移行や運用停止までの継続的な管理といった、ライフサイクル管理プロセス全体を自動化する。
- ソフトウェア スタック全体（オペレーティング システム、アプリケーション、パッチ、設定、およびコンテンツ）を自動的に展開し、望ましい状態になるように継続的に管理する。
- 異種またはスタンドアロン インフラストラクチャ内にある、デスクトップ コンピューター、ワークステーション、ノートブック コンピューターを含む、ほぼ任意のデバイスのソフトウェアを管理する。
- ほとんどのオペレーティング システム上でソフトウェアを管理する。

継続的な構成管理によって、HP のお客様からは、IT コストの大幅な削減、ソフトウェアやコンテンツを市場に投入するまでの時間の短縮、およびユーザーの生産性と満足度の向上が報告されています。

[HP Client Automation]ソリューションについて詳しくは、http://www.hp.com/go/client/（英語サイト）を参照してください。

HP Client Manager from Symantec

Altiris 社で開発された[HP Client Manager from Symantec]は、サポートされているすべての HP のビジネス向けデスクトップ コンピューター、ノートブック コンピューター、およびワークステーション モデルで無料で使用できます。SSM は、[HP Client Manager]に統合されており、HP クライアント システムのハードウェアの状態を中央から追跡、監視、および管理できるようにします。

[HP Client Manager from Symantec]を使用すると、以下のことが可能になります。

- CPU、メモリ、ビデオ、セキュリティ設定などの役立つハードウェア情報を取得する
- システム状態を監視して、問題が発生する前に解決できるようにする
- ドライバーおよび BIOS アップデートを、各 PC の場所まで移動しないで自動的に取得してインストールする
- BIOS やセキュリティ設定をリモートで設定する
- ハードウェアの問題を迅速に解決するためのプロセスを自動化する

HP Instant Support ツールに統合すると、ハードウェアの問題解決の時間を短縮できます。

- 診断：HP のデスクトップ、ノートブック、およびワークステーション モデルでレポートをリモートで実行および表示する
- システム状態のスキャン：HP クライアント システムの設置基盤での既知のハードウェア問題をチェックする
- アクティブ チャット：HP カスタマー サポートに問い合わせて問題を解決する
- HP ナレッジベース：専門的な情報にリンクする
- ハードウェアの問題を迅速に解決するための SoftPaq の自動的な収集および配信プロセス
- HP ProtectTools 内蔵セキュリティ チップを使用したシステムの認識、インベントリ、および初期化
- クライアント システムでシステム状態警告をローカルで表示するオプション
- HP 以外のクライアントの基本インベントリ情報のレポート
- TPM セキュリティ チップのセットアップと設定
- クライアントのバックアップとリカバリの集中スケジュール管理
- Intel AMT の管理用アドオン サポート

[HP Client Manager from Symantec]について詳しくは、http://www.hp.com/go/clientmanager/（英語サイト）を参照してください。

Altiris Client Management Suite

Altiris Client Management Suite は、デスクトップ、ノートブック、およびワークステーションのソフトウェアの全ライフサイクルを管理するための使いやすいソリューションです。Client Management Suite には以下の Altiris 製品が含まれています。

- Inventory Solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution
- Application Metering Solution

- Application Management Solution
- Carbon Copy Solution

Altiris Client Management Suite について詳しくは、http://www.symantec.com/business/client-management-suite（英語サイト）を参照してください。

HP Client Catalog for Microsoft System Center & SMS Products

[HP Client Catalog for Microsoft System Center & SMS Products]を使用すると、Microsoft 社製品を使用している IT 技術者は、HP のビジネス向けコンピューターへの HP ソフトウェア更新（SoftPaq）の配布を自動化できます。カタログ ファイルには、HP のビジネス向けデスクトップ コンピューター、ノートブック コンピューター、およびワークステーションの詳しいプラットフォーム情報が格納されています。このファイルを Microsoft 社製品のカスタム インベントリおよび更新機能とともに使用して、管理対象の HP クライアント コンピューターへのドライバーおよびパッチの更新を自動化できます。

[HP Client Catalog for Microsoft System Center & SMS Products]がサポートしている Microsoft 社製品は、以下のとおりです。

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server（SMS）2003 R2

[HP Client Catalog for SMS]について詳しくは、http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html（英語サイト）を参照してください。

リモート管理テクノロジ

モデルには、vPro テクノロジまたは標準テクノロジが搭載されています。このテクノロジを使用すると、ネットワークに接続したコンピューター アセットの検出、修復、および保護を適切に行うことができます。このテクノロジによって、システムがオンかオフか、またはオペレーティング システムが停止していないかどうかを管理できます。

ビジネス向けデスクトップ コンピューターで利用できるリモート管理機能の 3 つの形式は、ASF（Alert Standard Format）、Intel AMT（Active Management Technology）、および DASH（Desktop and mobile Architecture for Systems Hardware）です。

リモート管理テクノロジの機能には以下のものが含まれます。

- ネットワークの検出
- ハードウェア インベントリ情報
- プラットフォーム状態監視
- 電源管理：電源のオンとオフ、電源サイクル

- リモートの診断および修復
  - テキストコンソールリダイレクト：ブート フェーズ中のリモート PC のコンソール制御が可能
  - メディア リダイレクト：リモートの起動ドライブ、ディスク、または ISO イメージ（AMT プラットフォームの IDE リダイレクト（IDE-R）、および USB メディア リダイレクトの 2 種類がある）からシステムの起動が可能
- ハードウェア ベースの隔離とリカバリ：ウィルスのような動作が検出された場合に、PC ネットワークのアクセスを制限または切断
- プラットフォーム イベントの追跡と監査
- 統合 Web サーバー管理ポータルによるリモート アクセスおよび設定
- リモート管理テクノロジは、HP の管理コンソールパートナーに統合される

注記： 上記のすべての機能をすべてのプラットフォームで利用できるわけではありません。

Intel Management Engine の設定

注記： Intel vPro テクノロジの概要については、http://www.intel.com/jp/vpro/を参照してください。

Intel vPro テクノロジに関する HP 固有の情報については、http://www.hp.com/support/にあるホワイト ペーパーを参照してください。ホワイト ペーパーは英語で提供されていますので、**[United States (English)]**を選択し、**[See support and troubleshooting information]**（サポート&問題解決情報を表示する）をチェックしてからコンピューターのモデル番号を入力して Enter キーを押します。**[Resources for my selected product]**（選択した製品向けリソース）カテゴリで、**[Manuals (guides, supplements, addendums, etc)]**（マニュアル（ガイド、補足、付録など））をクリックします。**[Quick jump to manuals by category]**（カテゴリ別のマニュアルへのクイック ジャンプ）で、**[White papers]**（ホワイト ペーパー）をクリックします

使用可能なマネジメント テクノロジは以下のとおりです。

- AMT（DASH 1.0 を含む）
- ASF
- DASH 1.1（Broadcom NIC を使用）

ASF と AMT は同時に設定できませんが、どちらもサポートされています。

AMT または ASF の Intel vPro システムを設定するには、以下の手順で操作します。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[終了オプション]**（または**[シャットダウン]**）→**[再起動]**の順に選択します。
2. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に Ctrl ＋ P ホットキーを押します。

   注記： 適切なタイミングで Ctrl ＋ P キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 Ctrl ＋ P キーを押して、ユーティリティにアクセスします。

このホットキーで、Intel Management Engine BIOS Execution（MEBx）セットアップ ユーティリティが起動します。このユーティリティを使用すると、管理機能のさまざまな設定を行うことができます。構成オプションには、以下のものが含まれます。

- メイン メニュー
  - Intel ME Configuration（Intel ME の構成）
  - Intel AMT の構成
  - Change Intel ME Password（Intel ME パスワードの変更）
  - Exit（終了）
- Intel ME Platform Configuration（Intel ME プラットフォームの構成）
  - Intel ME State Control（Intel ME の状態制御）（有効/無効）
  - Intel ME Firmware Local Update（Intel ME ファームウェア ローカル アップデート）（有効/無効）
  - Intel ME Features Control（Intel ME の機能制御）
  - Intel ME Power Control（Intel ME の電源制御）
- Intel AMT の構成
  - Host Name（ホスト名）
  - TCP/IP
  - Provision Model（プロビジョニング モデル）（Enterprise、SMB）
  - Setup and Configuration（セットアップおよび構成）
  - Un-Provision（プロビジョニング解除）
  - SOL/IDE-R（有効/無効）
  - Password Policy（パスワード ポリシー）
  - Secure Firmware Update（ファームウェア アップデートのセキュリティ保護）（有効/無効）
  - Set PRTC（PRTC の設定）
  - Idle Timeout（アイドル タイムアウト）
- Intel ME パスワードの変更（このパスワードを変更することを強くおすすめします。初期設定のパスワードは「admin」です）

リモートで AMT システムを管理するには、管理者は AMT をサポートするリモート コンソールを使用する必要があります。エンタープライズ管理コンソールは、HP、Altiris、Microsoft SMS などのサプライヤーから入手できます。SMB モードでは、Web ブラウザー インタフェースがクライアントで提供されます。この機能にアクセスするには、ネットワーク上にある他の任意のシステムからブラウザーを開き、「http://host_name:16992」と入力します。host_name はシステムに割り当てられた名前です。また、ホスト名の位置に IP アドレスを使用することもできます。

Broadcom DASH 対応 NIC を搭載するシステムを設定するには、以下の操作を行います。

最新の資料を http://www.hp.com/jp/または http://www.hp.com（英語サイト）で確認します。**[サポート]→[トラブルシューティング]**の下でお使いの特定のモデルを選択した後、**[マニュアル]**を選択し、DASH または Broadcom NIC に関する**[ホワイトペーパー]**を選択します。

Verdiem Surveyor

Verdiem の[Surveyor]は PC のエネルギー費の管理に役立つソフトウェア ソリューションです。[Surveyor]は PC ごとの消費エネルギーを測定し、レポートします。また、PC の電源設定を制御できるため、管理者はネットワーク全体のエネルギー節減戦略を簡単に実装することができます。Surveyor エージェントを含む HP SoftPaq は、HP のサポート サイトからダウンロードして、サポート対象の市販デスクトップ モデルにインストールできます。PC を管理するための[Surveyor]のライセンスは、HP の担当窓口から購入できます。

HP Proactive Change Notification

Proactive Change Notification プログラムは、Subscriber's Choice の Web サイトを利用して、以下のことを事前にかつ自動的に行います。

- ほとんどの企業向け HP 製コンピューターおよびサーバーでハードウェアおよびソフトウェアの変更があった場合に、最も早くて 60 日前に電子メールで Proactive Change Notification（PCN）を通知する
- ほとんどの企業向け HP 製コンピューターおよびサーバーについての Customer Bulletins、Customer Advisories、Customer Notes、Security Bulletins、および Driver alerts を含んだ電子メールを送信する

特定の IT 環境に該当する情報のみを受け取るようにするため、ユーザー専用のプロファイルを作成します。HP Proactive Change Notification プログラムおよびカスタム プロファイルの作成について詳しくは、http://h30046.www3.hp.com/subhub.php（英語サイト）を参照してください。

Subscriber's Choice

Subscriber's Choice は HP のクライアントベースのサービスです。

ユーザーのプロファイルを基に、製品を使用する際のヒント、特集記事、およびドライバーやサポートに関する警告や通知を提供します。

Subscriber's Choice Driver and Support Alerts/Notifications では、購読するようプロファイルに設定した情報が閲覧および入手可能になると、電子メールで通知します。HP Subscriber's Choice およびカスタム プロファイルの作成について詳しくは、http://h30046.www3.hp.com/subhub.php（英語サイト）を参照してください。

廃止されたソリューション

Altiris Local Recovery と Dantz Retrospect の 2 つのソフトウェア パッケージは、今後 HP のビジネス向けデスクトップ コンピューター 、ノートブック、またはワークステーションには付属しません。

5 ROM フラッシュ機能

お使いのコンピューターでは、オペレーティング システムとの情報のやりとりなどを行う基本入出力システム（BIOS）がプログラム可能なフラッシュ ROM（読み取り専用メモリ）に記憶されています。[コンピューター セットアップ（F10）ユーティリティ]でセットアップ パスワードを設定しておけば、ROM の不用意な更新や上書きを防止できます。これは、コンピューターの動作の整合性を確保するために重要です。BIOS のアップグレードが必要な場合は、最新の BIOS イメージを HP のドライバーとサポートのページ http://www.hp.com/（英語サイト）からダウンロードできます。

△ **注意：** ROM を最大限に保護するために、必ずセットアップ パスワードを設定してください。セットアップ パスワードによって、ROM の不正なアップグレードを防止できます。[HP System Software Manager]を使用すると、システム管理者が、複数のコンピューターに同時にセットアップ パスワードを設定することができます。詳しくは、http://www.hp.com/go/ssm/（英語サイト）を参照してください。

リモート ROM フラッシュ機能

リモート ROM フラッシュ機能を利用すると、システム管理者は、ネットワーク管理端末からリモートでコンピューターの BIOS を安全に書き換えることができます。複数の HP のコンピューターに対してこのような作業をリモートで行うことができるので、ネットワーク上のコンピューターの BIOS を適切にアップグレードすることができます。さらに、生産性が向上し TCO（総所有コスト）を低減できます。

注記： Windows BitLocker Drive Encryption が有効になっていて、TPM 測定を使用しているシステムでは、BIOS をフラッシュすると、BitLocker がプラットフォーム用に作成した信頼署名が無効になります。そのため、このようなシステムの場合、BitLocker キーを保護するために、SSM では現在リモート ROM フラッシュがサポートされていません。システム BIOS をフラッシュするには、グループ ポリシーで BitLocker を無効にしてください。

リモート ROM フラッシュを使用するには、リモート ウェイク アップ機能を使用して、お使いのコンピューターの電源を入れておくか、再起動しておく必要があります。

リモート ROM フラッシュについて詳しくは、http://www.hp.com/go/ssm/（英語サイト）で[HP Client Manager Software]または[HP System Software Manager]を参照してください。

HPQFlash

HPQFlash ユーティリティは、Windows オペレーティング システムで個別のコンピューター上でシステム BIOS のアップデートや復元を行う場合に使用します。

HPQFlash について詳しくは、http://www.hp.com/にアクセスし、コンピューターのモデル番号を入力します。

6 Boot Block Emergency Recovery Mode

ROM フラッシュに失敗した場合に、Boot Block Emergency Recovery Mode によって、システム ROM を復旧またはアップグレードできます。たとえば、BIOS のアップグレード中に電源の障害が発生すると、ROM フラッシュは完了しないまま終了します。これによって、システム BIOS が使用不可能になります。Boot Block は、ROM フラッシュの際にも更新されない領域に収められており、コンピューターの電源投入時に有効なシステム BIOS イメージをチェックするコードが含まれています。

- システム BIOS イメージが有効な場合は、コンピューターは通常の方法で起動します。
- システム BIOS イメージが有効でない場合は、Boot Block BIOS によって、BIOS イメージ ファイル用のリムーバブル メディアを検索するための十分なサポートが提供されます。適切な BIOS イメージ ファイルが見つかると、そのファイルが ROM に自動的にフラッシュされます。

無効なシステム BIOS イメージが検出されると、システム電源ランプが 8 回赤く点滅します（1 秒間に 1 回の点滅）。同時に、スピーカーからビープ音が 8 回鳴ります。システム ROM の中の、ビデオ オプション ROM イメージが含まれている部分が壊れていなければ、画面に**[Boot Block Emergency Recovery Mode]**と表示されます。

Boot Block Emergency Recovery Mode になったら、以下のように操作して、システム BIOS を復旧（アップグレード）してください。

1. コンピューターの電源を切ります。
2. ルート ディレクトリに目的の BIOS イメージ ファイルが含まれている CD または USB フラッシュ デバイスを挿入します。

   注記： このメディアは、FAT12、FAT16、または FAT32 ファイル システムでフォーマットされている必要があります。

3. コンピューターの電源を入れます。

   適切な BIOS イメージ ファイルが見つからない場合は、BIOS イメージ ファイルが含まれているメディアを挿入するよう指示されます。

   システム BIOS の復旧またはアップグレードが正常に完了すると、システムによって電源が自動的に切られます。

4. BIOS のアップグレードに使用したリムーバブル メディアを取り出します。
5. 電源を入れて、コンピューターを起動しなおします。

注記： BIOS イメージ ファイルが含まれている CD がオプティカル ドライブに挿入されていると、BitLocker によって Windows Vista は起動できなくなります。BitLocker が有効になっている場合は、Windows Vista を起動する前に、この CD を取り出してください。

7 リプリケート セットアップ機能

以下のリプリケート セットアップ機能を使用すると、管理者がコンピューターの設定情報（コンフィギュレーション情報）を他の同じモデルのコンピューターに簡単にコピーすることができます。この機能によって、複数のコンピューターに同じ設定を行う時間を短縮することができます。

注記： これらの作業を行うには、ディスケット ドライブまたはサポートされる USB フラッシュ ドライブが必要です。

注記： [HP System Software Manager]（SSM）を使用すると、Windows オペレーティング システム内のコンピューター セットアップ情報を複製することができます。詳しくは、http://www.hp.com/go/ssm/（英語サイト）に掲載されている SSM のユーザー ガイドを参照してください。

1 台のコンピューターへのコピー

注意： 設定情報はモデルによって異なります。コピー元とコピー先のコンピューターが別のモデルの場合、ファイル システムが破損するおそれがあります。たとえば、dc7xxx シリーズのコンピューターから dx7xxx シリーズのコンピューターに設定情報をコピーしないでください。

1. 設定情報コピー元のコンピューターを選択します。コンピューターの電源を切ります。Microsoft Windows を実行している場合は、**[スタート]**→**[シャットダウン]**（または**[終了オプション]**）→**[シャットダウン]**（または**[電源を切る]**）の順に選択します。
2. 設定情報保存用ディスケットまたは USB フラッシュ メディア デバイスをここで挿入します。
3. コンピューターの電源を入れます。
4. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。

5. ディスケットを使用する場合はここで挿入します。
6. **[ファイル]**（File）→**[複製セットアップ]**（Replicated Setup）→**[リムーバブル メディアに保存]**（Save to Removable Media）の順に選択します。画面上のメッセージに沿って操作し、設定情報ディスケットまたは USB フラッシュ メディア デバイスを作成します。
7. 設定情報コピー先のコンピューターの電源を切り、設定情報ディスケットまたは USB フラッシュ メディア デバイスを挿入します。
8. 設定情報コピー先のコンピューターの電源を入れます。

9. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

10. **[ファイル]→[複製セットアップ]→[システム構成の復元]**（Restore from Removable Media）の順に選択した後、画面上のメッセージに沿って操作します。

11. 設定が完了したら、コンピューターを再起動します。

複数のコンピューターへのコピー

△ 注意： 設定情報はモデルによって異なります。コピー元とコピー先のコンピューターが別のモデルの場合、ファイル システムが破損するおそれがあります。たとえば、dc7xxx シリーズのコンピューターから dx7xxx シリーズのコンピューターに設定情報をコピーしないでください。

この手順では設定情報ディスケットまたは USB フラッシュ メディア デバイスの作成に少し時間がかかりますが、設定情報をコピー先のコンピューターにコピーする時間は大幅に短縮されます。

注記： この手順を行うため、また起動可能 USB フラッシュ メディア デバイスを作成するためには、起動可能ディスケットが必要です。起動可能ディスケットを作成するために Windows XP を使用できない場合は、1 台のコンピューターへのコピーの手順を実行してください（16 ページの 「1 台のコンピューターへのコピー」を参照）。

1. 起動可能ディスケットまたは USB フラッシュ メディア デバイスを作成します。18 ページの「サポートされる USB フラッシュ メディア デバイス」または19 ページの 「サポートされない USB フラッシュ メディア デバイス」を参照してください。

   △ 注意： USB フラッシュ メディア デバイスから起動できないコンピューターもあります。[コンピューター セットアップ（F10）ユーティリティ]に表示される初期設定の起動順序で、USB デバイスがハードディスク ドライブより前にある場合、そのコンピューターは USB フラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

2. 設定情報コピー元のコンピューターを選択します。コンピューターの電源を切ります。Microsoft Windows を実行している場合は、**[スタート]→[シャットダウン]**（または**[終了オプション]**）→**[シャットダウン]**（または**[電源を切る]**）の順に選択します。

3. 設定情報保存用ディスケットまたは USB フラッシュ メディア デバイスをここで挿入します。

4. コンピューターの電源を入れます。

5. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。

6. ディスケットを使用する場合はここで挿入します。

7. **[ファイル]**（File）→**[複製セットアップ]**（Replicated Setup）→**[リムーバブル メディアに保存]**（Save to Removable Media）の順に選択します。画面上のメッセージに沿って操作し、設定情報ディスケットまたは USB フラッシュ メディア デバイスを作成します。

8. [BIOS Utility for Replicated Setup]（リプリケート セットアップ用 BIOS ユーティリティ）をダウンロードして、この中に含まれる repset.exe ファイルを設定情報ディスケットまたは USB フラッ

シュ メディア デバイスにコピーします。このユーティリティを入手するには、http://welcome.hp.com/country/us/en/support.html（英語サイト）にアクセスし、コンピューターのモデル番号を入力します。

9. 設定情報ディスケットまたは USB フラッシュ メディア デバイス上で、以下のコマンドを含む autoexec.bat ファイルを作成します。

   repset.exe

10. 設定情報コピー先のコンピューターの電源を切ります。設定情報ディスケットまたは USB フラッシュ メディア デバイスを挿入し、コンピューターの電源を入れます。設定ユーティリティが自動的に実行されます。

11. 設定が完了したら、コンピューターを再起動します。

起動可能デバイスの作成

サポートされる USB フラッシュ メディア デバイス

サポートされるデバイスには、そのデバイスを簡単な手順で起動可能にするためのイメージがプリインストールされています。HP およびコンパックのすべての USB フラッシュ メディア デバイス、またその他のほとんどの USB フラッシュ メディア デバイスにこのイメージがプリインストールされています。使用している USB フラッシュ メディア デバイスにこのイメージが存在しない場合は、後で説明する手順に従ってください（「19 ページの 「サポートされない USB フラッシュ メディア デバイス」」を参照）。

起動可能な USB フラッシュ メディア デバイスを作成するには、以下のものが必要です。

- 対応する USB フラッシュ メディア デバイス
- FDISK および SYS プログラムが格納された、起動可能な DOS ディスケット（SYS がない場合は FORMAT を使用できますが、USB フラッシュ メディア デバイス上のファイルがすべて失われます）
- USB フラッシュ メディア デバイスから起動可能なコンピューター

△ **注意：** 一部の古いコンピューターでは、USB フラッシュ メディア デバイスから起動できない場合があります。[コンピューター セットアップ（F10）ユーティリティ]に表示される初期設定の起動順序で、USB デバイスがハードディスク ドライブより前にある場合、そのコンピューターは USB フラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

1. コンピューターの電源を切ります。
2. USB フラッシュ メディア デバイスをコンピューターの USB コネクタのどれかに差し込み、USB ディスケット ドライブ以外のすべての USB 記憶装置を取り外します。
3. FDISK.COM と、SYS.COM または FORMAT.COM のどちらかが格納された起動可能な DOS ディスケットをディスケット ドライブに挿入します。コンピューターの電源を入れて、DOS ディスケットを起動します。
4. **A:¥**プロンプトで「FDISK」と入力して Enter キーを押し、FDISK を実行します。メッセージが表示されたら、**[Yes]**（**[Y]**）をクリックして大容量ディスクのサポートを有効にします。
5. 選択肢の「5」を入力してコンピューターのドライブを表示します。一覧のドライブの中で最も容量が近いドライブが USB フラッシュ メディア デバイスで、通常は一覧の最後に表示されます。ドライブ名を書き留めておきます。

USB フラッシュ メディア デバイスのドライブ名：__________ __________

△ 注意： ドライブが USB フラッシュ メディア デバイスと一致しない場合は、データの損失を防ぐため、次の手順に進まないでください。他にストレージ デバイスがないか、すべての USB コネクタを確認します。あった場合は取り外してコンピューターを再起動し、手順 4 に進みます。ない場合、コンピューターが USB フラッシュ メディア デバイスに対応していないか、USB フラッシュ メディア デバイスが破損しています。この場合は USB フラッシュ メディア デバイスを起動可能にするための手順を実行しないでください。

6. Esc キーを押して **A:¥**プロンプトに戻り、FDISK を終了します。

7. 起動可能な DOS ディスケットに SYS.COM がある場合は手順 8 に、ない場合は手順 9 に進みます。

8. **A:¥**プロンプトで、「SYS x:」（x は書き留めたドライブ名）と入力します。

   △ 注意： USB フラッシュ メディア デバイスのドライブ名を正しく入力したことを確認します。

   システム ファイルの転送が完了すると、SYS から **A:¥**プロンプトに戻ります。手順 13 に進みます。

9. 保存しておきたいファイルを USB フラッシュ メディア デバイスから別のドライブ（コンピューターの内蔵ハードディスク ドライブなど）の一時ディレクトリにコピーします。

10. **A:¥**プロンプトで、「FORMAT /S X:」（X は書き留めたドライブ名）と入力します。

    △ 注意： USB フラッシュ メディア デバイスのドライブ名を正しく入力したことを確認します。

    FORMAT では 1 つ以上のメッセージが表示され、以下の手順に進む前に毎回確認画面が表示されます。毎回「Y」と入力します。FORMAT によって USB フラッシュ メディア デバイスがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。

11. ラベルを付けない場合は Enter キーを押し、必要な場合はラベルを入力します。

12. 手順 9 でコピーしたファイルを USB フラッシュ メディア デバイスにコピーしなおします。

13. ディスケットを取り出し、コンピューターを再起動します。USB フラッシュ メディア デバイスが C ドライブとして起動されます。

    注記： 初期設定の起動順序はコンピューターによって異なり、[コンピューター セットアップ（F10）ユーティリティ]で変更することができます。

    Windows 9x から DOS バージョンを使用した場合、短い間 Windows ロゴの画面が表示されることがあります。表示されないようにするには、USB フラッシュ メディア デバイスのルート ディレクトリに LOGO.SYS というゼロ長のファイルを追加します。

17 ページの 「複数のコンピューターへのコピー」に戻ります。

サポートされない USB フラッシュ メディア デバイス

起動可能な USB フラッシュ メディア デバイスを作成するには、以下のものが必要です。

- USB フラッシュ メディア デバイス
- FDISK および SYS プログラムが格納された、起動可能な DOS ディスケット（SYS がない場合は FORMAT を使用できますが、USB フラッシュ メディア デバイス上のファイルがすべて失われます）
- USB フラッシュ メディア デバイスから起動可能なコンピューター

△ **注意：** 一部の古いコンピューターでは、USB フラッシュ メディア デバイスから起動できない場合があります。[コンピューター セットアップ（F10）ユーティリティ]に表示される初期設定の起動順序で、USB デバイスがハードディスク ドライブより前にある場合、そのコンピューターは USB フラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

1. SCSI、ATA RAID、または SATA ドライブが取り付けられた PCI カードがコンピューターにある場合は、コンピューターの電源を切って電源コードを抜き取ります。

   △ **注意：** 電源コードは必ず抜き取ってください。

2. コンピューターのカバーを開いて PCI カードを取り外します。
3. USB フラッシュ メディア デバイスをコンピューターの USB コネクタのどれかに差し込み、USB ディスケット ドライブ以外のすべての USB 記憶装置を取り外します。コンピューターのカバーを閉じます。
4. 電源コードを差し込んでコンピューターの電源を入れます。
5. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。

6. **[カスタム]**（Advanced）→**[PCI デバイス]**（PCI Devices）の順に選択して PATA および SATA コントローラーを無効にします。SATA コントローラーを無効にするとき、コントローラーに割り当てられている IRQ を書き留めておきます。後で再び IRQ を割り当てる必要があります。変更を確定して、セットアップ ユーティリティを終了します。

   SATA IRQ : ___________ ___________

7. FDISK.COM と、SYS.COM または FORMAT.COM のどちらかが格納された起動可能な DOS ディスケットをディスケット ドライブに挿入します。コンピューターの電源を入れて、DOS ディスケットを起動します。
8. FDISK を実行して USB フラッシュ メディア デバイス上にあるパーティションをすべて削除します。新しいパーティションを作成して有効にします。Esc キーを押して FDISK を終了します。
9. FDISK を終了してもコンピューターが自動的に再起動されない場合は、Ctrl ＋ Alt ＋ Del キーを押して、DOS ディスケットから起動しなおします。
10. **A:¥**プロンプトで「FORMAT C:△/S」と入力し、Enter キーを押します。FORMAT によって USB フラッシュ メディア デバイスがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。
11. ラベルを付けない場合は Enter キーを押し、必要な場合はラベルを入力します。
12. コンピューターの電源を切って電源コードを抜き取ります。コンピューターのカバーを開き、取り外しておいた PCI カードを取り付けなおします。コンピューターのカバーを閉じます。
13. 電源コードを差し込み、ディスケットを取り出してコンピューターの電源を入れます。
14. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

15. **[カスタム]→[PCI デバイス]**の順に選択して、手順 6 で無効にした PATA および SATA コントローラーを再び有効にします。SATA コントローラーを元の IRQ に割り当てなおします。

16. 変更を保存してユーティリティを終了します。USB フラッシュ メディア デバイスが C ドライブとして起動されます。

注記： 初期設定の起動順序はコンピューターによって異なり、[コンピューター セットアップ（F10）ユーティリティ]で変更することができます。手順については、『コンピューター セットアップ（F10）ユーティリティ』を参照してください。

Windows 9x から DOS バージョンを使用した場合、短い間 Windows ロゴの画面が表示されることがあります。表示されないようにするには、USB フラッシュ メディア デバイスのルート ディレクトリに LOGO.SYS というゼロ長のファイルを追加します。

17 ページの 「複数のコンピューターへのコピー」に戻ります。

8　電源ボタン

お使いのコンピューターで ACPI（Advanced Configuration and Power Interface）を使用している場合は、電源ボタンをコンピューターのオン/オフ スイッチとしての機能のほか、スタンバイ モードを起動するためのボタンとして設定することができます。スタンバイ モードでは、電源を完全に切らずに、コンピューターの消費電力を低い状態に保つことができます。使用中のアプリケーションを終了しないで作業を途中で中断したい場合など、スタンバイ モードに設定しておくとコンピューターの電力を低く抑えることができます。

電源ボタンの設定を変更するには、以下の手順で操作します。

1. **[スタート]**ボタンをクリックし、**[コントロール パネル]**→**[パフォーマンスとメンテナンス]**→**[電源オプション]**の順に選択します。
2. **[電源オプションのプロパティ]**で**[詳細設定]**タブを選択します。
3. **[電源ボタン]**で**[スタンバイ]**を選択します。

電源ボタンにスタンバイ ボタンとしての機能を設定してある場合は、コンピューターの電源が入っているときに電源ボタンを押すと、スタンバイ モードを起動することができます。再び電源ボタンを押すと、直ちにスタンバイ モードから復帰できます。コンピューターの電源を完全に切るには、電源ボタンを 4 秒以上押し続けます。

△ **注意：**　システムが応答しない場合以外は、電源ボタンを使用して電源を切らないでください。オペレーティング システムを通さずに電源を切ると、ハードディスク ドライブが破損したりデータが損失したりする可能性があります。

9 HP Web サイト サポート

HP の技術者は HP 製および他社製のソフトウェアのテストおよび修正を厳密に行い、オペレーティング システムに特化したサポート ソフトウェアを開発しています。このため、HP のコンピューターは優れた性能、互換性、および信頼性を兼ね備えています。

別の種類のオペレーティング システムをインストールしたり新しいバージョンのオペレーティング システムに移行したりする場合、それぞれのオペレーティング システム用に設計されたサポート ソフトウェアを実行してください。お使いのコンピューターにインストールされているバージョンと異なるバージョンの Microsoft Windows を実行したい場合、対応するデバイス ドライバーおよびユーティリティをインストールして、すべての機能がサポートされ、正しく動作することを確認してください。

HP では、最新版のサポート ソフトウェアの検索、ダウンロード、インストールなどをより簡単に行えるようにしていきます。http://www.hp.com/support/からソフトウェアをダウンロードすることができます。

HP のホームページには、HP 製のコンピューターで Microsoft Windows のオペレーティング システムを実行する際に必要な最新のデバイス ドライバー、ユーティリティ、フラッシュ ROM イメージなどが用意されています。

10 業界標準

HP のインテリジェント マネジメント機能は、各社のシステム マネジメント アプリケーションを取り入れており、以下のようなコンピューター業界の標準規格に準拠しています。

- Web-Based Enterprise Management（WBEM）
- Windows Management Interface（WMI）
- Wake on LAN テクノロジ
- ACPI
- SMBIOS
- Pre-boot Execution（PXE）サポート

11 資産情報管理機能およびセキュリティ機能

コンピューターに搭載される資産情報管理機能を使用すれば、[HP Systems Insight Manager]、[HP Client Manager]、HP Configuration Management Solution、[HP Client Configuration Manager]、またはその他のシステム管理アプリケーションを使用して管理される資産情報を確認することができます。資産情報管理機能とこれらの管理ソフトウェア製品を統合することによって、お使いの環境に最適な管理ソフトウェアを選択でき、今までお使いになっていたソフトウェアをより有効に活用できます。

さらに、HP では、コンピューターとデータを不正なアクセスから保護するための機能を備えています。[Embeded Security for HP Protected Tools]がインストールされている場合は、データへの不正なアクセスの防止、システムの整合性の確認、および第三者からのアクセスに対する認証が行われます（詳しくは、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャー ガイド』を参照してください）。一部のモデルに装備されている[Embeded Security for HP Protected Tools]、スマート カバー センサー（Smart Cover Sensor）、スマート カバー ロック（Smart Cover Lock）などのセキュリティ機能は、パーソナル コンピューターの内部装置への不正なアクセスの防止に役立ちます。パラレル ポート、シリアル ポート、または USB コネクタを無効にすることによって、またリムーバブル メディア ブート機能を無効にすることによって、貴重な資産であるデータを保護できます。これ以外にも、メモリ脱着センサーおよびスマート カバー センサー/カバー リムーバル センサーからの警告が自動的にシステム管理アプリケーションに転送されることで、コンピューターの内部装置への不正なアクセスを防ぐことができます。

注記： [Embeded Security for HP Protected Tools]、スマート カバー センサー/カバー リムーバル センサー、およびスマート カバー ロックは、一部のシステムにオプションとして装備されています。

以下のユーティリティを使用して、セキュリティ機能の設定を管理できます。

- [コンピューター セットアップ（F10）ユーティリティ]を使用してローカルで管理します。[コンピューター セットアップ（F10）ユーティリティ]の詳しい情報と手順については、コンピューターに付属の Documentation and Diagnostics CD に収録されている『コンピューター セットアップ（F10）ユーティリティ ガイド』を参照してください。
- [HP Client Manager from Symantec]、[HP Client Automation]、または[HP System Software Manager]を使用してリモートで管理します。このソフトウェアによって、ネットワークのセキュリティ機能の設定を確実に、一貫して集中管理することができます。

以下の表と各項で、[コンピューター セットアップ（F10）ユーティリティ]を使用してローカルでコンピューターのセキュリティ機能を管理する方法を説明します。

表 11-1 セキュリティ機能

項目	説明

表 11-1 セキュリティ機能 (続き)

[セットアップ パスワード（Setup Password）]	セットアップ（管理者）パスワードを設定して有効にします 注記： セットアップ パスワードを設定すると、[コンピューター セットアップ（F10）ユーティリティ]の設定を変更したり、ROM をフラッシュしたり、Windows 環境で特定のプラグ アンド プレイ設定を変更したりする場合にセットアップ パスワードが必要になります
[電源投入時パスワード（Power-on Passowrd）]	電源投入時パスワードを設定して有効にします。電源を入れなおしたときに、電源投入時パスワードの入力画面が表示されます。ユーザーが正しい電源投入時パスワードを入力しない場合は、装置は起動されません 注記： 下の項目のパスワード オプションで有効にしない限り、Ctrl + Alt + Delete や Windows の手順によるウォーム ブート時には表示されません（下記を参照してください）
[パスワード オプション（Password Options）] （電源投入時パスワードまたはセットアップ パスワードが設定されている場合にのみ表示されます）	以下の項目を設定します ● レガシー リソースのロック（セットアップ パスワードを設定した場合に表示されます） ● ネットワーク サーバー モードを有効/無効に設定します（セットアップ パスワードを設定した場合に表示されます） ● ウォーム ブート（Ctrl + Alt + Delete）時にパスワードが必要かどうかを指定します（セットアップ パスワードを設定した場合に表示されます） ● 閲覧モードの設定を有効または無効に設定します（セットアップ パスワードを設定した場合に表示されます）（セットアップ パスワードを入力しない場合は、[コンピューター セットアップ（F10）ユーティリティ]のオプションを表示できますが、変更はできません） ● 厳重なパスワードを有効または無効に設定します（電源投入時パスワードを設定した場合に表示されます）。有効に設定すると、オンボード パスワード ジャンパーをスキップして、電源投入時パスワードを無効にします 詳しくは、『デスクトップ マネジメントについて』を参照してください
スマート カバー（Smart Cover）（一部のモデルのみ）	以下の項目を設定します ● カバー ロックのロックまたは解除 ● カバー リムーバル センサーの[無効]（Disable）/[ユーザーに通知]（Notify User）/[セットアップ パスワード]（Setup Password）への設定 注記： [ユーザーに通知]を設定すると、カバーが取り外されたことをセンサーが検知したときにユーザーに通知されます。[セットアップ パスワード]を設定すると、カバーが取り外されたことをセンサーが検知した場合、コンピューターを起動する際にセットアップ パスワードの入力が要求されます 一部のモデルでのみサポートされます
[デバイス セキュリティ（Device Security）]	以下のデバイスに関する、デバイス有効（Device Available）/デバイス無効（Device Hidden）を設定できます ● シリアル ポート（Serial Port） ● パラレル ポート（Parallel Port） ● 背面の USB ポート（Rear USB port） ● 前面の USB ポート（Front USB Port） ● 内蔵 USB ポート（Internal USB port） ● システム オーディオ（System audio） ● ネットワーク コントローラー（Network Controller） ● レガシー ディスケット（Legacy Diskette） ● 内蔵セキュリティ デバイス（Embedded security device）（一部のモデルのみ）

表 11-1 セキュリティ機能 (続き)

	● SATA0 ● SATA1（一部のモデルのみ） ● SATA2（一部のモデルのみ） ● SATA3（一部のモデルのみ） ● eSATA（一部のモデルのみ）
[LoJack for HP ProtectTools]	コンピューターをリモートから監視、管理、追跡できます [LoJack Pro for HP ProtectTools]はひとたび有効化されると、Absolute Software Customer Center から設定されます。管理者は Customer Center から[LoJack for HP ProtectTools]を設定し、コンピューターを監視または管理できます。システムの置き忘れや盗難が発生した場合、Customer Center はコンピューターを探索し取り戻すために地域当局をサポートすることができます。設定によって、ハードディスク ドライブが消去または交換された場合でも LoJack Pro が動作し続けるようにすることができます
[ネットワーク サービス ブート（Network Service Boot）]	ネットワーク サーバーにインストールされたオペレーティング システムからコンピューターを起動する機能を有効または無効にします（NIC（LAN ボード）が搭載されているモデルのみで使用でき、ネットワーク コントローラーが PCI 拡張カードであるか、システム ボードに組み込まれている必要があります）
[システム ID（System IDs）]	以下の項目を設定します ● アセット タグ（Asset Tag。18 バイトの ID）：会社によってコンピューターに割り当てられたプロパティ ID 番号 ● オーナーシップ タグ（Ownership Tag。80 バイトの ID）：POST 実行中に表示されます ● 本体シリアル番号（Chassis Serial Number）または UUID（Universal Unique Identifier）の入力。UUID は現在の本体シリアル番号が無効の場合にのみ更新できます（通常これらの識別（ID）番号は工場出荷時に設定され、そのシステムを特定するために使用されます） ● キーボード（Keyboard Locale）の設定：英語用やドイツ語用などをシステム ID エントリに対して設定します
[ドライブロック セキュリティ（DriveLock Security）]	ハードディスク ドライブにマスター パスワードまたはユーザー パスワードを割り当てたり、パスワードを変更したりします。この機能が有効の場合は、POST 実行中にどちらかのドライブロック パスワードを入力するよう求められます。どちらのパスワードも正常に入力されなかった場合は、次のコールド ブート シーケンスの間にどちらかのパスワードが入力されるまで、ハードディスク ドライブにはアクセスできません **注記：** この項目は、ドライブロック機能をサポートするハードディスク ドライブが少なくとも 1 台システムに接続されている場合にのみ表示されます

表 11-1 セキュリティ機能 (続き)

[セットアップのセキュリティ レベル（Setup Security Level）]	アクセスが制限されているエンド ユーザーが、セットアップ パスワードを知らなくても特定のセットアップ オプションを変更できる方法を提供します この機能を使用すると、エンド ユーザーがシステム設定を表示したり重要ではないオプションを変更したりできる状態でありながら、重要なセットアップ オプションへの変更を管理者が保護できるという柔軟性を得ることができます。管理者は、セットアップのセキュリティ レベルのメニューから、状況に応じて個々のセットアップ オプションへのアクセス権を設定できます。初期設定時には、すべてのセットアップ オプションにはセットアップ パスワードが割り当てられているため、任意のオプションを変更するには、ユーザーは POST 実行中に正しいセットアップ パスワードを入力する必要があります。管理者は個別の項目のセキュリティ レベルを「なし」に設定することもできますが、この場合、ユーザーがコンピューター セットアップ（F10）ユーティリティに不正なパスワードでアクセスしていたとしても、特定のオプションの値を変更できることになります。電源投入時パスワードが有効な場合は、**[なし]**を選択すると、電源投入時パスワードで置き換えられます **注記：** ユーザーがセットアップ パスワードを知らなくてもコンピューター セットアップ（F10）ユーティリティにアクセスできるようにするには、**[閲覧モードの設定]**（Set Up Browse Mode）を有効に設定する必要があります
システムのセキュリティ（System Security）（一部のモデルのみ：これらのオプションはハードウェア依存）	データ実行防止（Data Execution Prevention）（一部のモデルのみ）：有効/無効に設定します。オペレーティング システムのセキュリティの侵害を防止できます 仮想化技術（Virtualization Technology）（一部のモデルのみ）：有効/無効に設定します。プロセッサの仮想化機能を制御します。この設定を変更するには、コンピューターの電源を切ってから再び電源を入れる必要があります I/O 仮想化技術（Virtualization Technology Directed I/O）（一部のモデルのみ）：有効/無効に設定します。チップセットの仮想化 DMA リマップ機能を制御します。この設定を変更するには、コンピューターの電源を切ってから再び電源を入れる必要があります Trusted Execution Technology（一部のモデルのみ）：有効/無効に設定します。仮想アプライアンスをサポートするために必要な基礎プロセッサおよびチップセット機能を制御します。この設定を変更するには、コンピューターの電源を切ってから再び電源を入れる必要があります。この機能を有効にするには、以下の機能を有効に設定する必要があります ● 内蔵セキュリティ デバイスのサポート（Embedded Security Device Support） ● 仮想化技術（Virtualization Technology） ● I/O 仮想化技術（Virtualization Technology Directed I/O） 内蔵セキュリティ デバイスのサポート（Embedded Security Device Support）（一部のモデルのみ）：有効/無効に設定します。内蔵セキュリティ デバイスをアクティブまたは非アクティブにできます。この設定を変更するには、コンピューターの電源を切ってから再び電源を入れる必要があります **注記：** 内蔵セキュリティ デバイスを設定するには、セットアップ パスワードを設定する必要があります ● 工場出荷時設定へのリセット（Reset to Factory Settings）（一部のモデルのみ）：リセット（Reset）/リセットしない（Do not reset）に設定します。工場出荷時の初期値にリセットすると、すべてのセキュリティ キーが消去されます。この設定を変更するには、コンピューターの電源を切ってから再び電源を入れる必要があります **注意：** 内蔵セキュリティ デバイスは、多くのセキュリティ スキームの重要なコンポーネントです。セキュリティ キーを消去すると、内蔵セキュリティ デバイスによって保護されているデータへのアクセスができなくなります。[工場出荷時設定へのリセット]を選択すると、重要なデータの損失につながる可能性があります ● 認証資格情報のリセット（Reset authentication credentials）（一部のモデルのみ）：リセット（Reset）/リセットしない（Do not reset）に設定します。[リセット]を選択すると、電源投入時認証サポートが無効になり、内蔵セキュリティ デバイスからの認証情報が消去されます。この設定を変更するには、コンピューターの電源を切ってから再び電源を入れる必要があります

表 11-1 セキュリティ機能 (続き)

	OS による内蔵セキュリティ デバイス管理（OS management of Embedded Security Device）（一部のモデルのみ）: 有効/無効に設定します。このオプションを使用すると、内蔵セキュリティ デバイスの OS による制御を制限できます。この設定を変更するには、コンピューターの電源を切ってから再び電源を入れる必要があります。このオプションを設定すると、内蔵セキュリティ デバイスの OSによる制御を制限できます ● OS による内蔵セキュリティ デバイスのリセット（Reset of Embedded Security Device through OS）（一部のモデルのみ）: 有効/無効に設定します。このオプションを使用すると、内蔵セキュリティ デバイスの工場出荷時設定へのリセットを要求する OS の機能を制限できます。この設定を変更するには、コンピューターの電源を切ってから再び電源を入れる必要があります 注記： このオプションを有効にするには、セットアップ パスワードを設定する必要があります PAVP（一部のモデルのみ）: 無効（Disabled）/最小（Min）/最大（Max）に設定します。PAVP によってチップセットで Protected Audio Video Path が有効になります。このオプションによって、他の方法では再生できない、一部の保護されている高解像度コンテンツを表示できます。[最大]を選択すると、96 MB のシステム メモリが PAVP に専用に割り当てられます

パスワードのセキュリティ

電源投入時パスワード（Power-on password）を設定すると、コンピューターの電源を入れたり再起動したりするたびに、アプリケーションやデータにアクセスするためのパスワードの入力が要求されるので、コンピューターが許可無く使用されることを防止できます。セットアップ パスワード（Setup password）は、特に[コンピューター セットアップ（F10）ユーティリティ]への不正アクセスを防ぎます。セットアップ パスワードを、電源投入時パスワードの補助手段として使用することもできます。つまり、電源投入時パスワードの入力を要求されたときに、代わりにセットアップ パスワードを入力してコンピューターにアクセスすることもできます。

ネットワーク全体のセットアップ パスワードを設定しておくと、システム管理者はネットワーク上のすべてのシステムにログインでき、設定されている電源投入時パスワードを知らなくてもメンテナンスを行うことができます。

注記： [HP System Software Manager]（SSM）を使用すると、Windows オペレーティング システム内の BIOS パスワードを作成および管理することができます。詳しくは、http://www.hp.com/go/ssm/（英語サイト）に掲載されている SSM のユーザー ガイドを参照してください。

注記： [HP Client Management Interface]（HP CMI）を使用すると、BIOS パスワードを含む BIOS 設定管理に Windows オペレーティング システム内からアクセスすることができます。詳しくは、http://www.hp.com/go/hpcmi/（英語サイト）で[HP Client Management Interface]に関する技術ホワイトペーパーを参照してください。

セットアップ パスワードの設定

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャー ガイド』を参照してください。**[コンピューター セッ**

トアップ（F10）ユーティリティ]メニューで、セットアップ パスワードを設定しておけば、無断でコンピューターが再設定されることを防止できます。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]→[シャットダウン]→[再起動]**の順に選択します。
2. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。
3. **[セキュリティ]**（Security）→**[セットアップ パスワード]**（Setup Password）の順に選択した後、画面上のメッセージに従って操作します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

電源投入時パスワードの設定

[コンピューター セットアップ（F10）ユーティリティ]メニューで、電源投入時パスワードを設定しておけば、無断でコンピューターが使用されることを防止できます。電源投入時パスワードが設定されていると、[コンピューター セットアップ（F10）ユーティリティ]の**[セキュリティ設定]**（Security）メニューに**[パスワード オプション]**（Password Options）が表示されます。パスワード オプションには**[ウォーム ブート時のパスワード入力]**（Password Prompt on Warm Boot）などが含まれます。**[ウォーム ブート時のパスワード入力]**が有効にされている場合も、コンピューターを再起動するたびにパスワードを入力する必要があります。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]→[シャットダウン]→[再起動]**の順に選択します。
2. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。
3. **[セキュリティ]**（Security）→**[電源投入時パスワード]**（Power-On Password）の順に選択した後、画面上のメッセージに従って操作します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

電源投入時パスワードの入力

電源投入時パスワードを入力するには、以下の手順で操作します。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]→[シャットダウン]→[再起動]**の順に選択します。
2. 鍵形のアイコンが表示されたら、パスワードを入力して Enter キーを押します。

注記： 機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印の付いたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて 3 回間違えた場合は、コンピューターの電源をいったん切って最初から操作しなおす必要があります。

セットアップ パスワードの入力

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャー ガイド』を参照してください。

コンピューターでセットアップ パスワードを設定しておけば、[コンピューター セットアップ（F10）ユーティリティ]メニューを実行するたびに、必ずパスワードの入力が必要となります。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。
2. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10）]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。

3. 鍵形のアイコンが表示されたら、セットアップ パスワードを入力して Enter キーを押します。

   注記： 機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印の付いたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて 3 回間違えた場合は、コンピューターの電源をいったん切って最初から操作しなおす必要があります。

電源投入時パスワードまたはセットアップ パスワードの変更

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャー ガイド』を参照してください。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。
2. 電源投入時パスワードを変更する場合は、手順 3 に進みます。

   セットアップ パスワードを変更する場合は、コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押し、[コンピューター セットアップ（F10）]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。

3. 鍵形のアイコンが表示されたら、以下のように入力します。現在のパスワード/新しいパスワード/新しいパスワード

注記： 機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

4. Enter キーを押します。

新しいパスワードは、次にコンピューターの電源を入れたときから有効になります。

注記： 代替の区切り文字について詳しくは、32 ページの 「各国語キーボードの区切り文字」を参照してください。電源投入時パスワードとセットアップ パスワードは、[コンピューター セットアップ（F10）ユーティリティ]の**[セキュリティ]**（Security）オプションを使用して変更することもできます。

電源投入時パスワードまたはセットアップ パスワードの削除

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャー ガイド』を参照してください。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。

2. 電源投入時パスワードを削除する場合は、手順 3 に進みます。

   セットアップ パスワードを削除する場合は、コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押し、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。

3. 鍵形のアイコンが表示されたら、以下のように入力します。現在のパスワード/

4. Enter キーを押します。

   注記： 代替の区切り文字について詳しくは、32 ページの 「各国語キーボードの区切り文字」を参照してください。電源投入時パスワードとセットアップ パスワードは、[コンピューター セットアップ（F10）ユーティリティ]の**[セキュリティ]**（Security）オプションを使用して変更することもできます。

各国語キーボードの区切り文字

各キーボードは各国固有の要件に合うように設計されています。パスワードの変更または削除に使用する構文およびキーは、コンピューターに付属するキーボードによって異なります。

各国語キーボードの区切り文字					
/	アラビア語	-	ギリシャ語	/	ロシア語
=	ベルギー語	.	ヘブライ語	-	スロバキア語
-	BHCMSS*	-	ハンガリー語	-	スペイン語
/	ブラジル語	-	イタリア語	/	スウェーデン語/フィンランド語
/	中国語	/	日本語	-	スイス
-	チェコ語	/	韓国語	/	台湾語

各国語キーボードの区切り文字					
-	デンマーク語	-	ラテン アメリカ言語	/	タイ語
!	フランス語	-	ノルウェー語	.	トルコ語
é	カナダ フランス語	-	ポーランド語	/	アメリカ英語
-	ドイツ語	-	ポルトガル語		
* ボスニア ヘルツェゴビナ、クロアチア、モンテネグロ、セルビア、スロベニア					

パスワードの消去

設定しておいた電源投入時パスワードを忘れると、コンピューターを使用できなくなります。パスワードを解除する方法については、Documentation and Diagnostics CD に収録されている『トラブルシューティング ガイド』を参照してください。

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャー ガイド』を参照してください。

ドライブロック（DriveLock）

ドライブロックは、ATA ハードディスク ドライブにあるデータへの不正アクセスを防止する業界標準のセキュリティ機能です。[コンピューター セットアップ（F10）ユーティリティ]の拡張機能として実装されています。この機能は、ATA Security コマンド セットに対応するハードディスク ドライブが検出された場合にのみ利用できます。ドライブロックは、データのセキュリティを最重要視するユーザー向けに開発されました。このようなユーザーにとっては、ハードディスク ドライブのコストとそこに格納されているデータの喪失は、データへの不正アクセスの結果生じる可能性のある損害に比べれば、些細なものです。このレベルのセキュリティの確保と同時に、パスワードを忘れたときの対処もできるように、HP が実装したドライブロックでは、2 つのパスワードによるセキュリティ方式を採用しています。一方のパスワードはシステム管理者が設定して使用するもので、もう一方のパスワードは通常、エンド ユーザーが設定して使用します。両方のパスワードを忘れてしまった場合にドライブをアンロックするための手段はありません。したがって、ハードディスク ドライブに含まれるデータが企業情報システムに複製されているか、または定期的にバックアップが作成されている場合に、ドライブロックを最も安全に使用できます。ドライブロックの両方のパスワードを忘れてしまった場合は、ハードディスク ドライブを使用できなくなります。前に述べたカスタマー プロファイルに適合しないすべてのユーザーにとって、この事実は受け入れ難いリスクになる可能性があります。一方、カスタマー プロファイルに適合するユーザーにとっては、ハードディスク ドライブに保存されたデータの性質上、許容できるリスクだと言えます。

ドライブロックの使用法

ATA Security コマンド セットに対応するハードディスク ドライブが 1 つ以上検出された場合、[ドライブロック]（DriveLock）オプションが[コンピューター セットアップ（F10）ユーティリティ]の[セキュリティ]（Security）メニューに表示されます。ユーザーには、マスター パスワード（master password）を設定したりドライブロックを有効にしたりするオプションが提供されます。ドライブロックを有効にするには、ユーザー パスワード（user password）を入力する必要があります。通常、ドライブロックの最初のコンフィギュレーションはシステム管理者が実行するので、マスター パスワードを最初に設定する必要があります。ドライブロックを有効にするか無効のままにしておくかにかかわらず、管理者はマスター パスワードを設定することをおすすめします。これによって、将来ドライブがロックされた場合に、管理者はドライブロックの設定値を変更できるようになります。マスター パスワードが設定されると、システム管理者はいつでもドライブロックを有効にしたり無効にしたりすることができます。

ロックされたハードディスク ドライブが存在する場合は、POST（Power-On Self Test）によって、そのドライブをアンロックするためのパスワードが要求されます。電源投入時パスワード（power-on password）が設定されていて、そのドライブのユーザー パスワードと一致する場合は、パスワードの再入力は要求されません。一致しない場合は、ドライブロックのパスワードを入力するよう要求されます。コールド ブート時には、マスター パスワードとユーザー パスワードのどちらも使用することができます。ウォーム ブート時には、コールド ブートの前にドライブのロック解除に使用したパスワードと同じものを入力します。ユーザーは、パスワードが正しいと認識されるまで、2 回入力できます。コールド ブート時には、2 回とも受け入れられない場合でも POST は続行されますが、そのドライブにはアクセスできません。ウォーム ブート時または Windows からの再起動時には、2 回とも受け入れられない場合は POST が停止され、ユーザーは電源サイクルの指示に従います。

ドライブロックの使用例

ドライブロックのセキュリティ機能は、企業環境での使用に最も適しています。システム管理者はハードディスク ドライブのコンフィギュレーションを担当しますが、その作業には、ドライブロックのマスター パスワードおよび一時ユーザー パスワードを設定することが含まれます。ユーザーがユーザー パスワードを忘れた場合や、コンピューターを別の従業員が使用することになった場合、システム管理者はマスター パスワードを使用して、ユーザー パスワードをリセットしたり、ハードディスク ドライブへのアクセス権を回復したりすることができます。

企業システム管理者は、ドライブロックを有効にする場合、マスター パスワードの設定とメンテナンスについての企業方針を確立しておくことをおすすめします。これは、従業員が会社を辞める前に意図的に、または誤ってドライブロックの両方のパスワードを設定してしまうという状況を防ぐために必要です。両方のパスワードを設定した従業員が会社を辞めてしまった場合、そのハードディスク ドライブは使用不能となり、交換が必要になります。また、マスター パスワードが設定されていないと、システム管理者がロックされたハードディスク ドライブにアクセスできなくなり、不正ソフトウェアの日常チェックや、その他の資産管理およびサポートを実行できなくなることがあります。

それほど厳重なセキュリティを必要としないユーザーの場合は、ドライブロックを有効にしないことをおすすめします。この種のユーザーには、個人ユーザーや、機密性の高いデータをハードディスク ドライブに保持しないことを習慣にしているユーザーが含まれます。このようなユーザーにとっては、両方のパスワードを忘れてハードディスク ドライブが使用できなくなることの方が、ドライブロックによって保護されるデータの価値よりもはるかに大きな問題と言えます。[コンピューター セットアップ（F10）ユーティリティ]とドライブロックへのアクセスは、セットアップ パスワードによって制限できます。セットアップ パスワードを指定してそれをエンド ユーザーに公表しないことで、システム管理者はユーザーがドライブロックを有効にできないようにします。

スマート カバー センサー/カバー リムーバル センサー （Cover Removal Sensor）

一部のモデルに搭載されているスマート カバー センサー/カバー リムーバル センサーとは、本体のカバーまたはサイド パネルの着脱があったことをユーザーに知らせる、ハードウェア技術とソフトウェア技術を結合した機能です。3 段階の設定レベルがあり、本体のカバーの着脱があった後で初めてコンピューターの電源を入れたときの動作が異なります。

表 11-2 スマート カバー センサー/カバー リムーバル センサーの動作

Level	設定	説明
レベル 0	無効（Disabled）	スマート カバー センサー/カバー リムーバル センサーは無効（初期設定）
レベル 1	ユーザーに通知（Notify User）	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される。
レベル 2	セットアップ パスワード（Setup Password）	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される。セットアップ パスワードを入力するまで、コンピューターを使用できない

注記： これらの設定は、[コンピューター セットアップ（F10）ユーティリティ]を使用して変更できます。[コンピューター セットアップ（F10）ユーティリティ]について詳しくは、『コンピューター セットアップ（F10）ユーティリティ ガイド』を参照してください。

スマート カバー センサー/カバー リムーバル センサー（Cover Removal Sensor）の 保護レベルの設定

スマート カバー センサー/カバー リムーバル センサー機能を有効に設定するには、以下の手順で操作します。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。
2. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。
3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[カバー リムーバル センサー]**（Cover Removal Sensor）の順に選択した後、必要なセキュリティ レベルを選択します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

スマート カバー ロック

スマート カバー ロックは、コンピューターのカバーのロックをソフトウェアで制御する、一部の HP のコンピューターでサポートされる機能です。このロックによって、承認されていないユーザーによるコンピューター内部のコンポーネントへの不正なアクセスを防ぐことができます。工場出荷時には、ロックが解除された状態になっています。

△ **注意：** カバー ロック セキュリティを最大限にするために、必ずセットアップ パスワードを設定してください。セットアップ パスワードによって、[コンピューター セットアップ（F10）ユーティリティ]への不正なアクセスを防止できます。

注記： スマート カバー ロックは、一部のシステムにオプションとして装備されています。

スマート カバー ロックの設定

スマート カバー ロックを使用してコンピューター本体のカバーをロックするには、以下の手順で操作します。

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。

2. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。

3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[カバー ロック]**（Cover Lock）→**[ロック]**（Lock）の順に選択します。

4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

スマート カバー ロックの解除

1. コンピューターの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。

2. コンピューターの電源を入れたらすぐに、オペレーティング システムが起動する前に F10 キーを押して、[コンピューター セットアップ（F10)]ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピューターを再起動して、オペレーティング システムが起動する前にもう一度 F10 キーを押して、ユーティリティにアクセスします。

3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[カバー ロック]**（Cover Lock）→**[アンロック]**（Unlock）の順に選択します。

4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

Smart Cover FailSafe キーの使用

スマート カバー ロックを使用してコンピューターをロックしたまま、パスワードを入力できなくなってしまった場合、Smart Cover FailSafe キーを使用して、コンピューター本体のカバーを開ける必要があります。Smart Cover FailSafe キーが必要となるのは、以下のような場合です。

- 停電
- 起動障害

- コンピューター部品（プロセッサや電源など）の障害
- パスワードを忘れてしまった場合

△ **注意：** Smart Cover FailSafe キーは、HP が提供する専用ツールです。このキーが必要になる前に、HP 製品販売店であらかじめご用意いただくことをおすすめします。

FailSafe キーを入手するには、以下のどちらかを行います。

- HP のサポート窓口にお問い合わせください。
- 保証書に記載されている適切な番号に連絡します。

Smart Cover FailSafe キーについて詳しくは、『ハードウェア リファレンス ガイド』を参照してください。

セキュリティ ロック ケーブル用スロット

コンピューターのリア パネルにはロック ケーブルを取り付けられるようになっている（一部のモデルのみ）ので、市販のロック ケーブルを使用して、コンピューターを作業エリアに固定できます。

詳しくは、『ハードウェア リファレンス ガイド』を参照してください。

指紋認証テクノロジ

HP 指紋認証テクノロジを使用すると、エンド ユーザーのパスワードの入力が不要となるため、ネットワークのセキュリティを強化する一方で、ログイン手順を簡素化し、企業のネットワーク管理に関わる経費を削減することができます。また、手頃な価格のため、もはや一部のハイテク産業や高度なセキュリティを扱う組織や企業だけのものではなくなりました。

注記： モデルによっては、指紋認証テクノロジがサポートされていない場合があります。

障害通知および復旧機能

障害通知および復旧機能とは、最新のハードウェア/ソフトウェア技術を結合して、重要なデータの損失を防ぎ、故障時間を最小限に抑える機能です。

HP Client Manager によって管理されるネットワークにコンピューターが接続されている場合、ネットワーク管理ソフトウェアに障害通知が送られます。HP Client Manager Software では、管理されているすべてのコンピューターで診断ユーティリティを実行し、失敗したテストの概要を作成するよう、リモートでスケジュールを設定することもできます。

ドライブ保護システム

ドライブ保護システム（DPS）は、一部のモデルに搭載されたハードディスク ドライブに組み込まれている診断ツールです。DPS を使用して、保証規定が適用されない、ハードディスク ドライブの交換に至るような問題を診断します。

HP コンピューターの組み立て時に各ハードディスク ドライブに対して DPS テストが実行され、主要な情報がハードディスク ドライブに書き込まれます。この情報は半永久的に記録されます。DPS が実行されるたびに、テストの結果がハードディスク ドライブに書き込まれます。サポート窓口では、この情報を基に、DPS ソフトウェアを実行する原因となった状況を特定できます。DPS の使用方法については、『トラブルシューティング ガイド』を参照してください。

耐サージ機能付連続供給電源装置

耐サージ機能が付いた連続供給電源によって、急激な電圧の変化に対処することができます。この電源装置は、データの損失やシステム ダウンを引き起こさずに 2000 V までのサージ電圧に耐えられることが確認されています。

温度センサー機能

温度センサー機能は、ハードウェアとソフトウェアの統合によって提供される機能で、コンピューター内部の温度を監視します。温度が通常の範囲を超えると、画面上に警告メッセージが表示されるため、内部部品の故障やデータの損失が発生する前に対処することができます。

△ **注意：** 高温状態は、システムの損傷やデータの損失につながるおそれがあります。

索引